PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2002-152271
(43) Date of publication of application : 24.05.2002

(51) Int.Cl. H04L 12/56
G06F 17/30
H04L 12/28

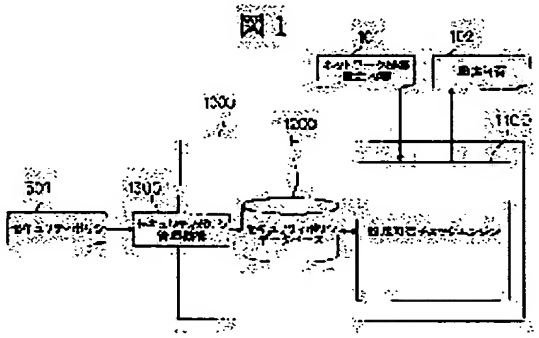
(21) Application number : 2001-109398
(22) Date of filing : 09.04.2001

(71) Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72) Inventor : KOMIYA TERUYUKI
FUJI HITOSHI

(30) Priority
Priority number : 2000265058 Priority date : 01.09.2000 Priority country : JP

(54) SECURITY POLICY HIGH-SPEED RETRIEVAL METHOD, DEVICE AND RECORDING MEDIUM RECORDED WITH PROGRAM THEREFOR

(57) Abstract:
PROBLEM TO BE SOLVED: To provide a security policy high-speed retrieval method and device that can suppress increasing rate of a retrieval time, with respect to the increase in setting items and the increase in an entry registered as a security policy.
SOLUTION: The security policy high-speed retrieval method and device has a security policy storage procedure, that stores security policy possessed by a network manager to a computer system and a setting propriety check procedure, that checks the propriety of setting request for a network device, on the basis of the security policy.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－152271
（P2002－152271A）
(43)公開日　平成14年５月24日(2002.5.24)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｚ	５Ｂ０７５
Ｇ０６Ｆ　17/30	１７０	Ｇ０６Ｆ　17/30	１７０Ｚ	５Ｋ０３０
Ｈ０４Ｌ　12/28	２００	Ｈ０４Ｌ　12/28	２００Ｚ	５Ｋ０３３

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－109398(P2001－109398)
(22)出願日　平成13年４月９日(2001.4.9)
(31)優先権主張番号　特願2000－265058(P2000－265058)
(32)優先日　平成12年９月１日(2000.9.1)
(33)優先権主張国　日本（ＪＰ）

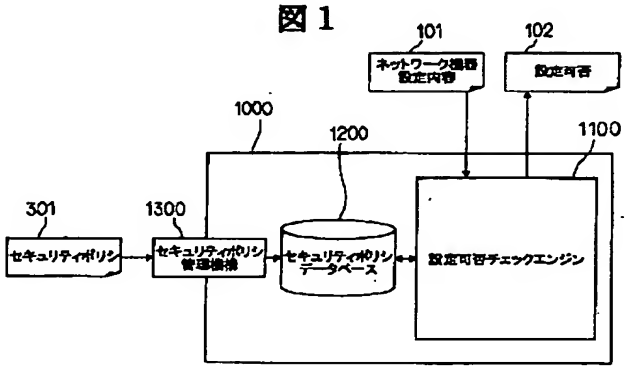
(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　小宮　輝之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　冨士　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　セキュリティポリシ高速検索方法、装置及びそのプログラムを記録した記録媒体

(57)【要約】
【課題】　設定を行う項目の増加やセキュリティポリシとして登録されるエントリの増加に対して、検索時間の増加率を抑える。
【解決手段】　ネットワーク管理者が保持しているセキュリティポリシをコンピュータシステムに保持するセキュリティポリシ保持手順と、ネットワーク機器の設定要求をセキュリティポリシによって設定の可否をチェックする設定可否チェック手順とを有することを特徴とするセキュリティポリシ高速検索方法および装置。

図１



1

【特許請求の範囲】

【請求項１】　ネットワーク管理者が保持しているセキュリティポリシをコンピュータシステムに保持するセキュリティポリシ保持手順と、
ネットワーク機器の設定要求をセキュリティポリシによって設定の可否をチェックする設定可否チェック手順とを有することを特徴とするセキュリティポリシ高速検索方法。

【請求項２】　前記セキュリティポリシは、一つの機器の設定に必要な項目の組に対して、許可された設定内容をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与されることを特徴とする請求項１に記載のセキュリティポリシ高速検索方法。

【請求項３】　前記セキュリティポリシ保持手順は、パケットフィルタリングにおけるソース側ＩＰアドレス範囲とデスティネーション側ＩＰアドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれをｘ軸、ｙ軸上にマッピングした平面図形として表現し、セキュリティポリシとして登録されたエントリの数をＮとしたときに、与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断する処理時間のオーダがＯ（Ｎ）以下となるデータ構造を用いることを特徴とする請求項１に記載のセキュリティポリシ高速検索方法。

【請求項４】　前記設定可否チェック手順は、２次元データ検索を行う２次元データ検索手順と、検索対象を管理する検索対象管理手順とからなることを特徴とする請求項１乃至３のうちいずれか１項に記載のセキュリティポリシ高速検索方法。

【請求項５】　前記２次元データ検索手順は、前記のセキュリティポリシのデータ構造を用いて、前記判断に対する処理時間が、セキュリティポリシとして登録されたエントリの数をＮとしたときの処理時間のオーダＯ（Ｎ）以下の処理時間で検索処理を行うことを特徴とする請求項４に記載のセキュリティポリシ高速検索方法。

【請求項６】　前記検索対象管理手順は、セキュリティポリシの中で検索対象となるエントリの識別子を管理する手順であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除くことを特徴とする請求項４又は５に記載のセキュリティポリシ高速検索方法。

【請求項７】　ネットワーク管理者が保持しているセキュリティポリシをコンピュータシステムに保持するセキュリティポリシ保持手段と、ネットワーク機器の設定要求をセキュリティポリシによって設定の可否をチェックする設定可否チェック手段とを有することを特徴とするセキュリティポリシ高速検索装置。

【請求項８】　前記セキュリティポリシは、一つの機器の設定に必要な項目の組に対して、許可された設定内容

2

をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与される手段であることを特徴とする請求項７に記載のセキュリティポリシ高速検索装置。

【請求項９】　前記セキュリティポリシ保持手段は、パケットフィルタリングにおけるソース側ＩＰアドレス範囲とデスティネーション側ＩＰアドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれをｘ軸、ｙ軸上にマッピングした平面図形として表現し、セキュリティポリシとして登録されたエントリの数をＮとしたときに、与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断する処理時間のオーダがＯ（Ｎ）以下となるデータ構造であることを特徴とする請求項７に記載のセキュリティポリシ高速検索装置。

【請求項１０】　前記設定可否チェック手段は、２次元データ検索を行う２次元データ検索手段と、検索対象を管理する検索対象管理手段とからなることを特徴とする請求項７乃至９のうちいずれか１項に記載のセキュリティポリシ高速検索装置。

【請求項１１】　前記２次元データ検索手段は、前記のセキュリティポリシのデータ構造を用いて、前記判断に対する処理時間が、セキュリティポリシとして登録されたエントリの数をＮとしたときの処理時間のオーダＯ（Ｎ）以下の処理時間で検索処理を行う手段であることを特徴とする請求項１０に記載のセキュリティポリシ高速検索装置。

【請求項１２】　前記検索対象管理手段は、セキュリティポリシの中で検索対象となるエントリの識別子を管理する手段であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除く手段であることを特徴とする請求項１０又は１１に記載のセキュリティポリシ高速検索装置。

【請求項１３】　請求項１乃至請求項６のいずれか１項に記載のセキュリティポリシ高速検索方法の処理手順を、コンピュータに実行させるためのプログラムを記録したコンピュータ読み出し可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、仮想閉域網（ＶＰＮ：Virtual Private Network）製品などのネットワーク機器を利用して、ネットワークを介して通信を行うことによって作られる論理閉域網に関し、特に、前もって定めたセキュリティポリシに基づいてネットワーク機器の設定内容の設定可否をチェックする際に、高速にチェックを行う方法及び装置に関する。

【０００２】

【従来の技術】ネットワーク上に、物理的なネットワーク構成に依存しない論理閉域網を構成するには、パケットフィルタリング（以下、Ｐ．Ｆ．と称する）やＶＰＮ

等いくつものネットワーク機器を設定する。ネットワーク管理者は、各ネットワーク機器の、ＩＰ（Internet Protcol）アドレスやポート番号など設定すべき複数の項目全てに関して、設定内容がネットワークの属する組織の方針であるセキュリティポリシの範囲内であるかどうかを調べ、設定を許可するかどうかを判断する。このとき、ネットワーク管理者は、設定内容がセキュリティポリシの範囲内かをチェックするために、複数の項目ごとに、事前に登録されたセキュリティポリシのうち該当する項目のエントリ全体に対して検索を行う。

【０００３】

【発明が解決しようとする課題】前記従来の技術では、設定内容がセキュリティポリシの範囲内かをチェックするための検索時間は、設定を行う項目の増加、及びセキュリティポリシとして登録されるエントリの増加に比例して長くなる。ネットワークが大規模化することは、一般に、設定を行うネットワーク機器の増加やセキュリティポリシとして登録するエントリの増加が伴うため、従来の技術では困難になる。また、きめ細かいセキュリティポリシを定義することも、セキュリティポリシとして登録するエントリの増加が伴うため、従来の技術では困難になる。本発明は、前記従来技術の問題点を解決するためになされたものであり、本発明の目的は、設定を行う項目の増加やセキュリティポリシとして登録されるエントリの増加に対して、検索時間の増加率を抑えることが可能な技術を提供することにある。本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述及び添付図面によって明らかにする。

【０００４】

【課題を解決するための手段】本願において開示される発明の概要を簡単に説明すれば、下記のとおりである。ここでいう、ネットワーク利用者とは、通信を行うコンピュータなどをネットワークに接続し、そのコンピュータを使用する人物であり、ネットワーク機器とは、コンピュータが通信を行うネットワークに接続されている機器やソフトウェアである。また、ネットワーク管理者とは、ネットワーク利用者が利用できるコンピュータやサービスの決定など、ネットワーク機器の管理方針を作成し、ネットワーク機器の設定を行う人物である。また、論理閉域網とは、ゲートウェアやファイアウォールなどで物理的に他のネットワークと切り離されている物理ネットワークに制限されることなく、特定のコンピュータなどだけが通信できるように、情報に特定の識別子を付与したり、特定の鍵による暗号化を施すことによって実現するネットワークである。

【０００５】本発明は、ネットワーク管理者が保持しているセキュリティポリシをコンピュータシステムに保持しておくセキュリティポリシ保持手段と、ネットワーク機器の設定要求をセキュリティポリシによって設定の可否をチェックする設定可否チェック手段とからなるセキュリティポリシ高速検索方法及び装置である。

前記セキュリティポリシ保持手段では、セキュリティポリシは、一つの機器の設定に必要な項目の組に対して、許可された設定内容をあてはめたものを一単位とし、この単位ごとに一意な識別子が付与される。

【０００６】さらに、Ｐ．Ｆ．におけるソース（source）側ＩＰアドレス範囲とデスティネーション（destination）側ＩＰアドレス範囲のように二つの設定値範囲として扱えるものは、一つの設定項目として扱い、それぞれをｘ軸、ｙ軸上にマッピングした平面図形として表現し、ウィンドウ質問（与えられた長方形が、すでに存在する長方形と部分的に重なる、または含まれるかどうかを判断することを、一般にウィンドウ質問と呼ぶ）に対する処理時間がＯ（Ｎ）以下となるデータ構造を用いる。ここで、Ｏ（Ｎ）は、セキュリティポリシとして登録されたエントリの数をＮとしたときの処理時間のオーダを表し、Ｎが増加するときに、処理時間が一次関数で増加することを意味する。ウィンドウ質問に対する処理時間がＯ（Ｎ）以下となるデータ構造として、領域４分木やＭＸ－ＣＩＦ４分木、Ｒ木などが挙げられる。

【０００７】前記設定可否チェック手段は、２次元データ検索を行う２次元データ検索手段と検索対象を管理する検索対象管理手段からなり、この二つの手段によって高速な検索を実現する。前記２次元データ検索手段は、前記のセキュリティポリシのデータ構造を用いてＯ（Ｎ）以下の処理時間で検索処理を行う手段である。前記検索対象管理手段は、セキュリティポリシの中で検索対象となるエントリの識別子を管理する手段であり、複数の設定項目に対して検索処理を行う際に、他の項目の検索結果から、検索が不要と判断されるエントリの識別子を検索対象から取り除くことで、全てのエントリに対して検索を行う場合よりも高速な検索を実現する。また、前記セキュリティポリシ保持手段におけるデータ構造が、２次元データ検索を行う前にあらかじめ一部の検索対象を除外することが困難なデータ構造の場合であっても、一般に、セキュリティポリシのチェックにあたる平面図形同士の比較よりも、識別子の比較の処理時間の方が小さいため、より高速な検索が実現できる。

【０００８】ネットワーク管理者は、セキュリティポリシをコンピュータシステムにデータとして保存しておく。ここでのコンピュータシステムを、以下では、セキュリティポリシ検索装置と呼び、データをセキュリティポリシデータベースと呼ぶ。ネットワーク管理者が、ネットワーク利用者から要求された論理閉域網の構成条件をもとに導出したネットワーク機器の設定要求をセキュリティポリシ検索装置に入力すると、セキュリティポリシ検索装置は、セキュリティポリシで許可されている範囲かをチェックし、設定の可否を出力する。

【０００９】

【発明の実施の形態】以下、図面を参照して本発明の実

施の形態を詳細に説明する。なお、実施の形態を説明するための全図において、同一機能を有するものは同一符号を付け、その繰り返しの説明は省略する。図１は、本発明による一実施形態（実施例）のセキュリティポリシ検索装置の概略構成を示す模式図である。図１において、１０００はセキュリティポリシ検索装置、１０１はネットワーク機器設定内容、１０２はネットワーク機器設定内容１０１に対する設定可否、３０１はセキュリティポリシ、１１００はネットワーク管理者からのネットワーク機器設定内容１０１を受付けて設定可否１０２を導出する設定可否チェックエンジン、１２００はセキュリティポリシ３０１を保存するセキュリティポリシデータベース、１３００はネットワーク管理者からのセキュリティポリシ３０１を受付けてセキュリティポリシデータベース１２００を更新するセキュリティポリシ管理機構である。

【００１０】図１に示すように、本実施形態（実施例）のセキュリティポリシ検索装置１０００は、ネットワーク管理者からのネットワーク機器設定内容１０１を受付けて設定可否１０２を導出する設定可否チェックエンジン１１００と、セキュリティポリシ３０１を保存するセキュリティポリシデータベース１２００とで構成される。前記セキュリティポリシ３０１について、Ｐ．Ｆ．におけるソース側ＩＰアドレス範囲とデスティネーション側ＩＰアドレス範囲、ソース側ポート範囲とデスティネーション側ポート範囲、アドレス変換におけるプライベート（private）側ＩＰアドレス範囲とグローバル（global）側ＩＰアドレス範囲、ＶＰＮにおけるソース側ＩＰアドレス範囲とデスティネーション側ＩＰアドレス範囲、及びソース側ポート範囲とデスティネーション側ポート範囲は、二つの設定値範囲を一組として扱い、それぞれをｘ軸、ｙ軸上にマッピングした平面図形として表現する。

【００１１】前記Ｐ．Ｆ．、及びＶＰＮにおけるソース側ＩＰアドレス範囲とデスティネーション側ＩＰアドレス範囲“（ｓｒｃ_ｉｐ．ｆｒｏｍ～ｓｒｃ_ｉｐ．ｔｏ）→（ｄｓｔ_ｉｐ．ｆｒｏｍ～ｄｓｔ_ｉｐ．ｔｏ）”は、ｓｒｃ_ｉｐ．ｆｒｏｍ～ｓｒｃ_ｉｐ．ｔｏ間の任意のＩＰアドレスをソース側アドレスとし、ｄｓｔ_ｉｐ．ｆｒｏｍ～ｄｓｔ_ｉｐ．ｔｏ間の任意のＩＰアドレスをデスティネーション側アドレスとするＩＰアドレス対を指す。一つのＩＰアドレス対は、２次元平面上の、一つの長方形として表現される（図２）。ただし、ｓｒｃ_ｉｐ．ｆｒｏｍ≦ｓｒｃ_ｉｐ．ｔｏ、及びｄｓｔ_ｉｐ．ｆｒｏｍ≦ｄｓｔ_ｉｐ．ｔｏの条件が成り立っているとする。

【００１２】前記Ｐ．Ｆ．、及びＶＰＮにおけるソース側ポート範囲とデスティネーション側ポート範囲“（ｓｒｃ_ｐｏｒｔ．ｆｒｏｍ～ｓｒｃ ｐｏｒｔ．ｔｏ）→（ｄｓｔ ｐｏｒｔ．ｆｒｏｍ～ｄｓｔ ｐｏｒｔ．ｔｏ）”は、ｓｒｃ ｐｏｒｔ．ｆｒｏｍ～ｓｒｃ ｐｏｒｔ．ｔｏ間の任意のポートをソース側ポートとし、ｄｓｔ ｐｏｒｔ．ｆｒｏｍ～ｄｓｔ ｐｏｒｔ．ｔｏ間の任意のポートをデスティネーション側ポートとするポート対を指す。一つのポート対は、２次元平面上の、一つの長方形として表現される。ただし、ｓｒｃ_ｐｏｒｔ．ｆｒｏｍ≦ｓｒｃ_ｐｏｒｔ．ｔｏ、及びｄｓｔ_ｐｏｒｔ．ｆｒｏｍ≦ｄｓｔ_ｐｏｒｔ．ｔｏの条件が成り立っているとする。

【００１３】アドレス変換におけるプライベート（private）側ＩＰアドレス範囲とグローバル（global）側ＩＰアドレス範囲“（ｐｒｉｖａｔｅ_ｉｐ．ｆｒｏｍ～ｐｒｉｖａｔｅ_ｉｐ．ｔｏ）⇒（ｇｌｏｂａｌ_ｉｐ．ｆｒｏｍ～ｇｌｏｂａｌ_ｉｐ．ｔｏ）”は、ｐｒｉｖａｔｅ_ｉｐ．ｆｒｏｍ～ｐｒｉｖａｔｅ_ｉｐ．ｔｏ間のＩＰアドレス（プライベート側）から、ｇｌｏｂａｌ_ｉｐ．ｆｒｏｍ～ｇｌｏｂａｌ_ｉｐ．ｔｏ間のＩＰアドレス（グローバル側）への対応を定義したアドレス変換対を指す。一つのアドレス変換対は、表１に示すようにアドレス変換の種類（名称はＲＦＣ２６６３“ＩＰ Network Address Translator（ＮＡＴ）Terminology and Considerations”の定義による）によって、２次元平面上で図３に示す図形として表現される。ただし、ｐｒｉｖａｔｅ_ｉｐ．ｆｒｏｍ≦ｐｒｉｖａｔｅ_ｉｐ．ｔｏ、及びｇｌｏｂａｌ_ｉｐ．ｆｒｏｍ≦ｇｌｏｂａｌ_ｉｐ．ｔｏの条件が成り立っているとする。

【００１４】

【表１】

アドレス変換の種類と図形の形状

アドレス変換の種類		図形の形状
Two-Way NAT	Static NAT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、private_ip.to-private_ip.from =global_ip.to-global_ip.from
Traditional NAT	Basic NAT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、private_ip.to-private_ip.from =global_ip.to-global_ip.from
	NAPT	線分(private_ip.from, global_ip.from)-(private_ip.to, global_ip.to) ただし、global.from=global.to

ネットワーク機器設定内容１０１について、Ｐ．Ｆ．やアドレス変換、ＶＰＮに関するネットワーク機器設定内容は、セキュリティポリシ３０１と同様、二つの設定値範囲を一組として扱い、それぞれをｘ軸、ｙ軸上にマッピングした平面図形として表現する。

【００１５】図４は、セキュリティポリシ検索装置１０

００の状態遷移を示す図であり、図５は、前記セキュリティポリシ検索装置１０００の処理手順を示すフローチャートである。前記セキュリティポリシ検索装置１０００の処理手順は、図５に示すように、まず、初期状態において、ネットワーク管理者が、セキュリティポリシ３０１を定め、セキュリティポリシ管理機構１３００からセキュリティポリシ検索装置１０００へ入力することで、セキュリティポリシデータベース１２００へ新規追加を行う（ステップ２０１）。

【００１６】この状態以降は、ステップ２０２での処理内容の判定に基づき、ネットワーク管理者が、セキュリティポリシ３０１を定め、セキュリティポリシ管理機構１３００からセキュリティポリシ検索装置１０００へ入力することによる、セキュリティポリシデータベース１２００の更新処理（ステップ２０３）、及びネットワーク管理者が、ネットワーク機器設定内容１０１を定め、設定可否チェックエンジン１１００へ入力することによる、設定可否１０２の導出処理（ステップ２０４）が任意に行われる。また、ステップ２０３での更新処理の後に、セキュリティポリシデータベース１２００が空か否かを判断し（ステップ２０５）、セキュリティポリシデータベース１２００が空の場合、即ち、ネットワーク管理者が、セキュリティポリシ管理機構１３００からセキュリティポリシ検索装置１０００へ指示することで、セキュリティポリシデータベース１２００を全て削除した場合には初期状態に戻り、セキュリティポリシ検索装置１０００は、ネットワーク機器設定内容１０１を受付けることはできなくなる。

【００１７】図６は、前記設定可否チェックエンジン１１００の処理手順を示すフローチャートである。前記設定可否チェックエンジン１１００の処理手順は、図６に示すように、まず、前記設定可否チェックエンジン１１００は、ネットワーク管理者からネットワーク機器設定内容１０１の入力を受付ける（ステップ２１１）。次に、入力されたネットワーク機器設定内容１０１の種類が判断され（ステップ２１２）、ステップ２１２での判断結果に基づき、入力されたネットワーク機器設定内容１０１の種類に対応した設定可否チェックを行い（ステップ２１３～ステップ２１５）、設定可否１０２を求める。そして、設定可否チェックエンジン１１００は、設定可否１０２の内容をネットワーク管理者へ返す（ステップ２１６）。

【００１８】図７は、前記設定可否チェックエンジン１１００で行われる設定可否チェックの処理手順を示すフローチャートである。前記設定可否チェックの処理は、図７に示すように、設定可否チェックエンジン１１００に入力されたネットワーク機器設定内容１０１を設定要求Ｒとし、Ｒがセキュリティポリシデータベース１２００で管理されているセキュリティポリシＰによって許可されているかのチェックを行い、その結果を設定可否１０２として出力する。また、設定不可の場合には、“設定不可”と、設定許可と判断された設定値のリストと、設定不可と判断された設定値のリストを出力する。ネットワーク管理者は、受取った設定可否結果１０２が設定可であった場合、一般には入力したネットワーク機器の設定内容１０１の設定を行う。また、受取った設定可否結果１０２が設定不可であった場合、ネットワーク管理者は、入力したネットワーク機器の設定内容１０１のうち設定可と判断された部分だけの設定を行う、もしくはネットワーク機器の設定内容１０１を破棄する。

【００１９】前記設定可否チェックの処理手順は、図７に示すように、初めに、ネットワーク機器設定内容１０１の設定要求Ｒが入力されると（ステップ２２１）、ｊ＝１とし（ステップ２２２）、次に、対象リストの初期値として、１からｎの値を設定するとともに不可リストを空集合とする（ステップ２２３）。ここで、対象リストは、セキュリティポリシＰのうち、検索対象となるＰｉを指す識別子ｉの集合である。セキュリティポリシＰとして登録されたエントリは、必ずしも一つではなく、複数存在する場合もある（数１の式）。なお、このＰｉにおいて、ｉが本発明の識別子に相当する。ここで、設定要求Ｒ＝｛ＲＣ1，ＲＣ2，・・・ＲＣj，・・・，ＲＣm｝、セキュリティポリシＰｉ＝｛Ｃi1，Ｃi2，・・・，Ｃij，・・・，Ｃim｝とし、ＲＣｊとＣijはＩＰアドレスやポート番号などの設定項目である。

【００２０】

【数１】

$$(P=\sum_{i=1}^{n} Pi)$$

そこで、対象リストに識別子が含まれるＣｊ（数２の式）からＲＣｊの平面検索を行い（ステップ２２５）、ＲＣｊ（ｘ）∧￢Ｃｊ（ｘ）となるｘが存在するか否かを判断し（ステップ２２６）、ステップ２２６でＮｏの場合は、ステップ２２８に進み、ステップ２２６でＹｅｓの場合には、許可されない設定値の項目をその許可されない値で置き換えたＲを、不可リストへ加える（ステップ２２７）。次に、ＲＣｊと部分的に重なる、又は、ＲＣｊを含むＣijを指す識別子ｉのみを対象リストに残す（ステップ２２８）。前述のステップ２２５からステップ２２８までのセキュリティによるチェック処理は、ステップ２２４と、ステップ２２９及びステップ２３０により、Ｒの各項目ＲＣｊ（ｊ=1，2，・・・，ｍ）全てについて調べる。

【００２１】Ｒの全項目が調べ終わった時点で、不可リストが空集合か否かを判断し（ステップ２３１）、ステップ２３１で、不可リストが空集合のままの場合には、全てのＲＣｊがセキュリティポリシによって許可されたと判断し、”設定可”を出力する（ステップ２３４）。ステップ２３１で、不可リストが空集合ではない場合に

は、Ｒから不可リストの設定値を取り除いたものを許可リストとし（ステップ２３２）、”設定不可”、許可リスト、不可リストを出力する（ステップ２３３）。ステップ２２５での、ＲＣｊの設定値が、セキュリティポリシの一部分であるＣｊ（数２の式）によって許可されて

$$Cj=\sum_{i=1}^{n} Cij$$

図形ＲＣｊ上にある全ての点ｘが、図形集合Ｃｊに含まれる図形の少なくとも一つの図形Ｃｉｊと重なっていれば、図形ＲＣｊで表現される設定要求は、セキュリティポリシによって設定することが許可されていると判断する。これは、数３の式の真偽値を判定することと等しい。ＲＣｊ（ｘ）∧¬Ｃｊ（ｘ）となるｘが存在しなければ真、つまり図形Ｒで表現される設定要求はセキュリティポリシによって設定することが許可されていると判断する。この処理を行うためには、まず、ＲＣｊと部分的に重なる、またはＲＣｊを含むＣｉｊを検索する必要がある。この検索は、前述のようにＣｉｊのデータ構造として領域４分木などのデータ構造を用いることで、Ｃ１ｊからＣｎｊまでのそれぞれとの比較した場合よりも高速に行うことが可能である。

【００２３】

【数３】∀ｘ（ＲＣｊ（ｘ）→Ｃｊ（ｘ））≡¬∃ｘ¬（ＲＣｊ（ｘ）→Ｃｊ（ｘ））≡¬∃ｘ¬（¬ＲＣｊ（ｘ）∨Ｃｊ（ｘ））≡¬∃ｘ（ＲＣｊ（ｘ）∧¬Ｃｊ（ｘ））

ＲＣｊ（ｘ）∧¬Ｃｊ（ｘ）が存在しない：ＲＣｊが意味する設定要求は設定可能

ＲＣｊ（ｘ）∧¬Ｃｊ（ｘ）が存在する　：ＲＣｊが意味する設定要求は設定不可

（数３の式のセキュリティポリシによる設定可否チェック）

ＲＣ１に関するセキュリティポリシのチェックの検索対象は、Ｃ１１からＣｎ１の全てとし、ＲＣ（ｊ+1）に関するセキュリティポリシのチェックの検索対象は、ＲＣｊに関するセキュリティポリシのチェックの検索において、ＲＣｊと部分的に重なる、又はＲＣｊを含むＣｉｊのｉに相当するＣｉ（ｊ+1）のみとする。ｊが増加するにつれて検索対象が絞られるため、ＲＣｊのそれぞれにおいてＣ１ｊからＣｎｊの全てを対象として検索を行う場合よりも高速に検索を行うことが可能である。前記設定要求ＲＣｊとセキュリティポリシＣｉｊの関係を図８に示す。

【００２４】図９は、前記セキュリティポリシ管理機構１３００の処理手順を示すフローチャートである。前記セキュリティポリシ管理機構１３００は、ネットワーク管理者からセキュリティポリシ３０１の入力を受付け（ステップ２４１）、受付けたセキュリティポリシ３０１の処理内容を判断し（ステップ２４２）、その処理内容をもとにセキュリティポリシデータベース１２００の削除（ステップ２４３）、更新（ステップ２４４）、あるいは追加（ステップ２４５）を行う。なお、前記各処理は、コンピュータ上で動作するコンピュータプログラムによっても実現可能であり、前記各処理を実行するコンピュータプログラムは、コンピュータが読み取り可能な記録媒体で提供される。ここで、コンピュータ読み取り可能な記録媒体とは、フロッピー（登録商標）ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記録装置をいう。以上、本発明者によってなされた発明を、前記実施の形態に基づき具体的に説明したが、本発明は、前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【００２５】

【発明の効果】本願において開示される発明によって得られる効果を簡単に説明すれば、下記のとおりである。本発明によれば、ネットワーク機器の設定内容が、セキュリティポリシによって許可されているかを高速に検索する手段を設けたので、設定を行う項目の増加やセキュリティポリシとして登録されるエントリの増加に対して、検索時間の増加率を抑えることができる。これにより、ネットワークを大規模化や、きめ細かいセキュリティポリシの定義を行うことができる。

【図面の簡単な説明】

【図１】本発明による一実施形態（実施例）のセキュリティポリシ検索装置の概略構成を示す模式構成図である。

【図２】本実施形態のＩＰアドレス対の表現を示す図である。

【図３】本実施形態のアドレス変換対の表現を示す図である。

【図４】本実施形態のセキュリティポリシ検索装置の状態遷移図である。

【図５】本実施形態のセキュリティポリシ検索装置の処理手順を示すフローチャートである。

【図６】本実施形態の設定可否チェックエンジンの処理手順を示すフローチャートである。

【図７】本実施形態の設定可否チェック処理手順を示すフローチャートである。

【図８】本実施形態の設定要求とセキュリティポリシの関係を示す図である。

11

【図９】本実施形態のセキュリティポリシ管理機構のセキュリティポリシによる設定可否チェック処理手順を示すフローチャートである。

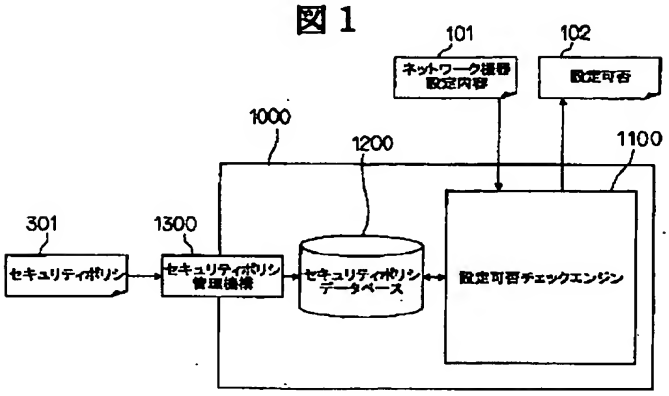
【符号の説明】

１０００…セキュリティポリシ検索装置、１１００…設定可否チェックエンジン、１２００…セキュリティポリシデータベース、１３００…セキュリティポリシ管理機構、１０１…ネットワーク機器設定内容、１０２…設定可否、３０１…セキュリティポリシ。

12

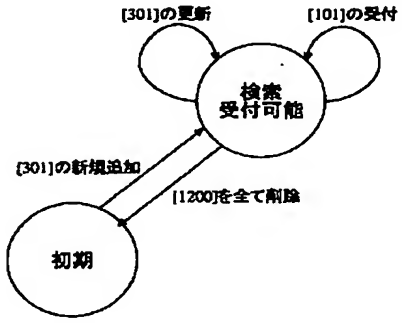
【図１】

図 1



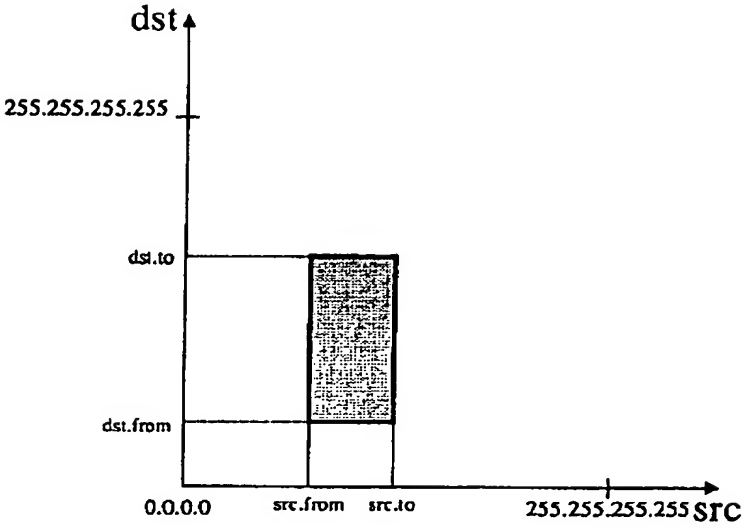
【図４】

図 4



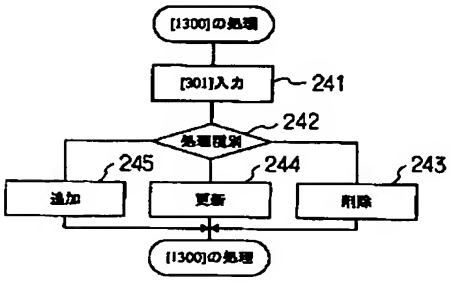
【図２】

図 2



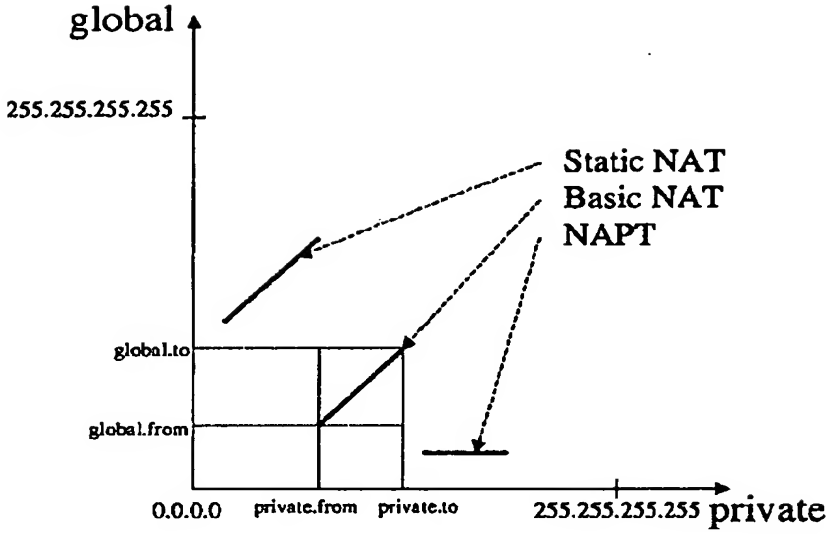
【図９】

図 9



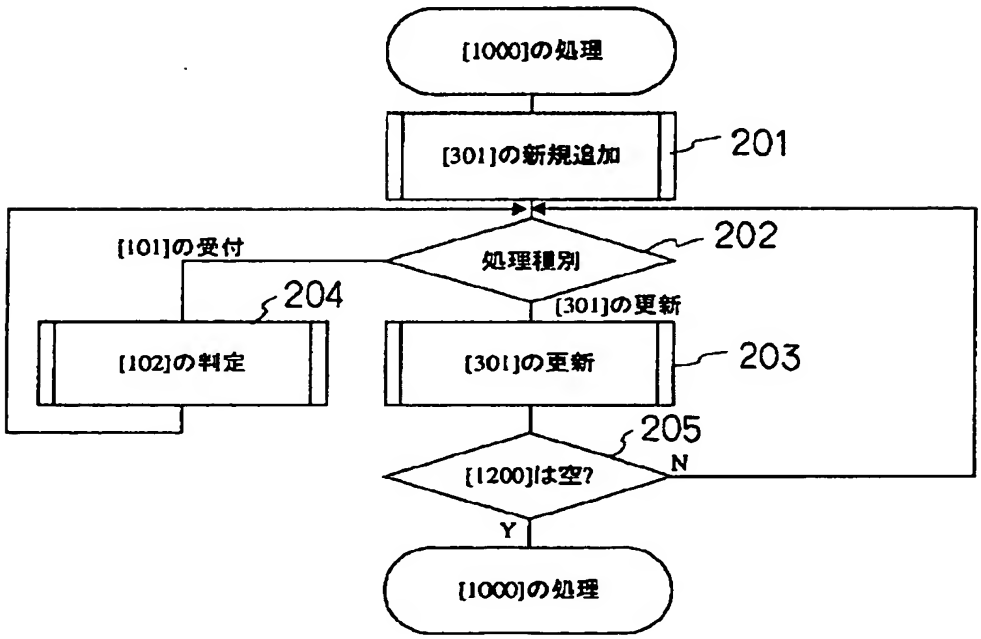
【図３】

図 3


global
255.255.255.255
Static NAT
Basic NAT
NAPT
global.to
global.from
0.0.0.0
private.from
private.to
255.255.255.255
private

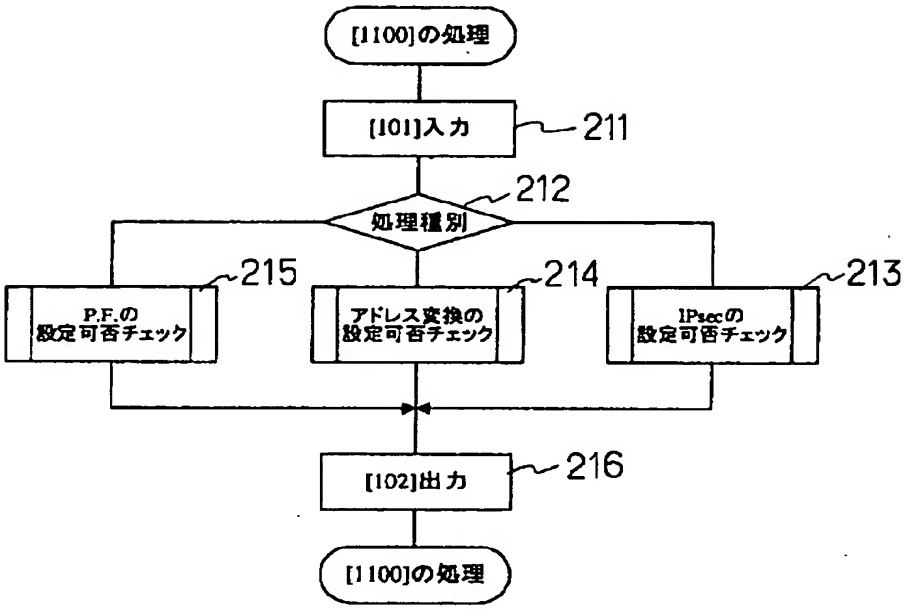
【図５】

図 5


[1000]の処理
[301]の新規追加
201
[101]の受付
処理種別
202
[301]の更新
204
[102]の判定
[301]の更新
203
205
[1200]は空?
N
Y
[1000]の処理

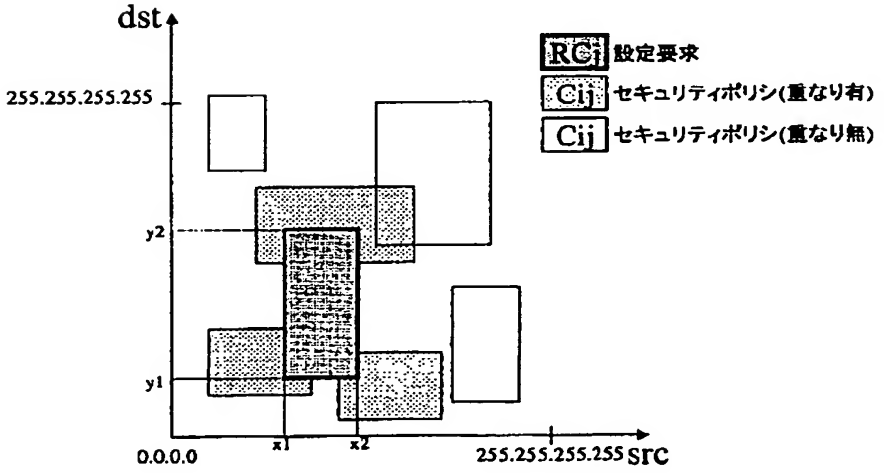
【図６】

図 6


[1100]の処理
[101]入力
211
212
処理種別
215
214
213
P.F.の
設定可否チェック
アドレス変換の
設定可否チェック
IPsecの
設定可否チェック
[102]出力
216
[1100]の処理

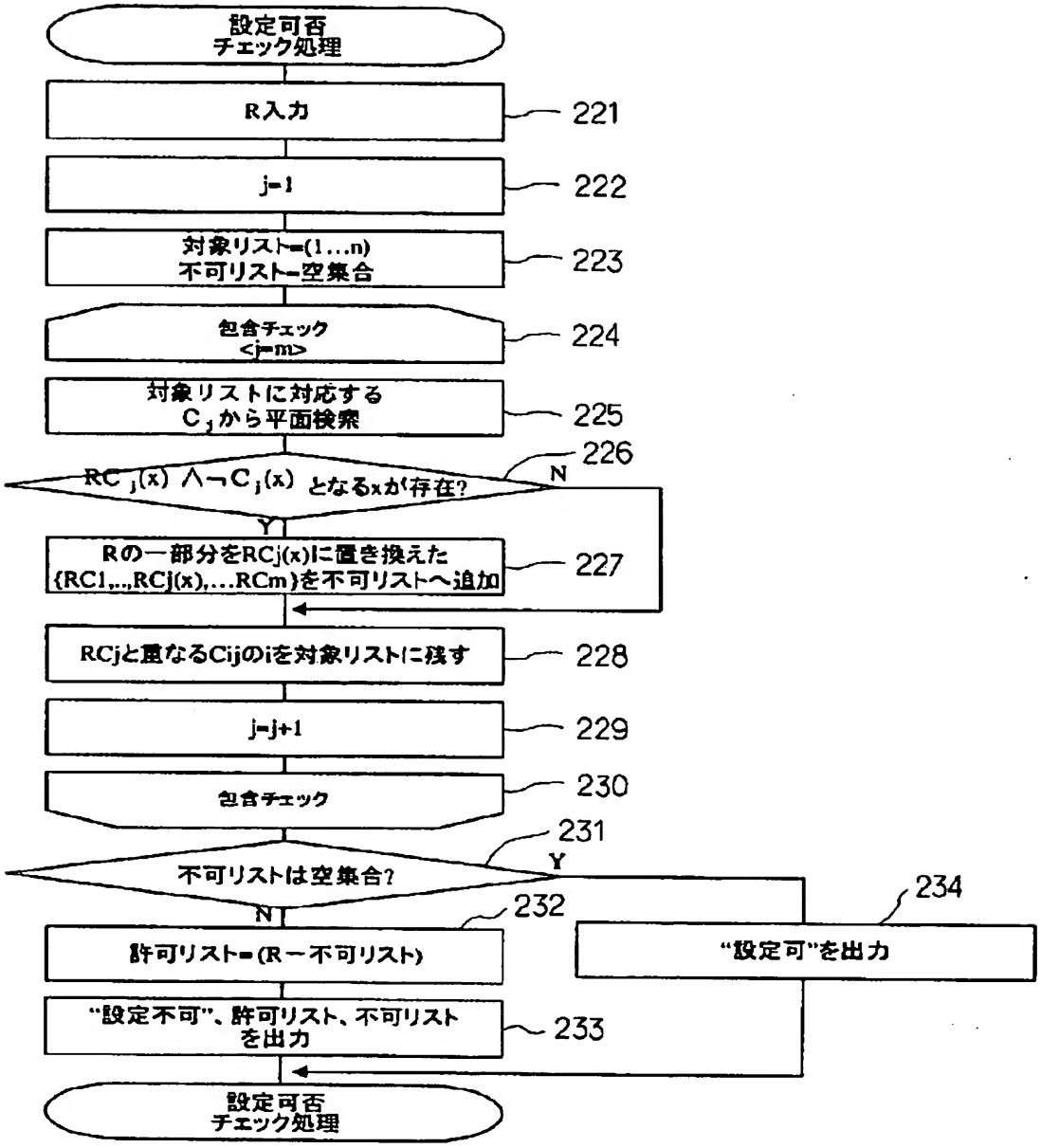
【図８】

図 8


dst
255.255.255.255
y2
y1
0.0.0.0
x1
x2
255.255.255.255
src
RCi
設定要求
Cij
セキュリティポリシ(重なり有)
Cij
セキュリティポリシ(重なり無)

【図７】

図 7



フロントページの続き

Ｆターム(参考) 5B075 KK02 KK43 KK70 UU40
5K030 GA15 HA08 HB08 HB19 HD09
KA07 LB05 LC13 LD17
5K033 AA08 BA08 CB09 CC01 DB12
DB14